UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,414	03/03/2004	Jing Xiang	NRT.0124US	2562

21906 7590 08/06/2008

TROP PRUNER & HU, PC
1616 S. VOSS ROAD, SUITE 750
HOUSTON, TX 77057-2631

EXAMINER	
TABOR, AMARE F	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
08/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/791,414	XIANG ET AL.	
	Examiner	Art Unit	
	AMARE TABOR	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-12,14,17 and 20-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7, 9-12, 14, 17 and 20-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on May 27, 2008, **prosecution is hereby reopened**.

2. A new ground of rejection is set forth below.

3. To avoid abandonment of the application, appellant must exercise one of the following two options: (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or, (2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

4. A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

5. Claims 8, 13, 15, 16, 18 and 19 are cancelled.

6. **Claims 1-7, 9-12, 14, 17 and 20-22** are pending.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Ahonen" (US 2001/0009025 A1, now US 6,976,177 B2), in view of Bahl et al. (US 7,020,464 B2 – "Bahl")

As per Claim 1, Ahonen teaches,

A method for maintaining secure network connections [see *Fig.1-5 and abstract;* and for example, *par.0004 to 0011]*, the method comprising: detecting a change of address from an old address to a new address associated with a first network element [see *the mobile host 1 in Fig.1*; and for example *par.*

0010, 0012, 0098, 0109, 0111 to 0113, 0124, 0129, 0133 and 0134]; updating at least one first security configuration at the first network element [see *Fig.2-4 and abstract; where the authentication certificate is updated at the mobile host*; and for example, *par. 0006-0011 and 0019-0023*]; and transmitting at least one secure message from the first network element to a second network element [see *Fig.2-4; where secure messages, such as: ISKAMP SA, IPSec SA #1/#2, Proposal, etc. are transmitted between Peer 1/Initiator and Peer 2/Responder*].

Ahonen teaches the at least one secure message contains the new address [see for example, *par.0097-0105 and 0111-0118*] - *where the control authorization certificate sent from the mobile host to the firewall consists the (New) Source and Destination addresses (if changed)*], wherein the new address in the at least one secure message enables at least one second security configuration at the second network element to be updated [see *Fig.5; and where certificate is sent from mobile host to firewall, and firewall authorizes mobile host*; and for example, *Remote Control Function form par.0108-0129*]; but fails to teach wherein the at least one secure message contains both the old address and the new address, wherein the old address and the new address in the at least one secure message enables at least one second security configuration at the second network element to be updated.

However, in the same filed of endeavor, **Bahl** teaches at least one secure message contains both the old address and the new address, wherein the old address and the new address in the at least one secure message enables at least one second security configuration at the second network element to be updated [see abstract, "*…The mobile host sends an address change message to each of its correspondent hosts over a secured control channel and preferably through* ***a tunnel created based on the old and new addresses***. *Upon receiving the notification, the correspondent host returns an acknowledgment through the control channel and modifies its security filters…*"]. Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify the system of **Ahonen** by incorporating the teaching of **Bahl** in order to handle the network communications between a mobile device and other computing devices when the network address of the mobile device changes [see at least abstract of **Bahl**].

As per Claim 9, Ahonen-Bahl combination teaches,

At least one processor readable-medium for storing a computer program of instructions configured to be readable by at least one processor for instructing the at least one processor to execute a computer process for performing the method as recited in claim 1 [see *Fig.2-5 and abstract;* and for example, *par.0019-0023 and 0035*] *of* ***Ahonen****; and FIGS.1-3 of* ***Bahl*** *where means for storing computer program instructions/"daemons" and inherent processor in the mobile host or security gateway/firewall and server/correspondent host are disclosed*].

As per Claim 2, Ahonen-Bahl combination teaches,

wherein a lookup of security associations is not dependent on any destination address [*the Remote Control Database/RCDB is within the firewall, is not dependent on the destination address*; see for example, *par.0012, 0106 and 0119-0122 of* ***Ahonen***].

As per Claim 3, Ahonen-Bahl combination teaches,

wherein the first network element is a mobile client and the second network element is a security gateway [see *mobile host 1 and security gateway 3 in Fig.1 of* ***Ahonen***].

As per Claim 4, Ahonen-Bahl combination teaches,

wherein the first network element and the second network element are part of a virtual private network (VPN) [see *abstract and Fig.1;* and for example, *par.0001, 0005, 00013 and 0029 of* ***Ahonen***].

As per Claim 5, Ahonen-Bahl combination teaches,

wherein communications between the first network element and the second network element are based on a security architecture for the internet protocol (IPsec); and wherein communications between the mobile client and the first security server are based on a security architecture for the internet protocol (IPsec) [see *SAs based on IPSec in Fig.2 and 4 of* ***Ahonen***].

As per Claim 6, Ahonen-Bahl combination teaches,

wherein at least part of the communications between the first network element and the second network element are based on an internet security association and key management protocol (ISAKMP) [see *SA based on ISAKMP in Fig.2 of* ***Ahonen***].

As per Claim 7, Ahonen-Bahl combination teaches,

the second network element identifying at least one security association based on at least one cookie field in the at least one secure message [see for example, *par.0055, 00119-0127 and 0133-0137 of* ***Ahonen****; where the second network element; i.e., the firewall, identifies the SA based on the cookie field*].

Claims 10, 11, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Ahonen", in view of Coile et al. (US 6,108,300– "Coile")

As per Claim 10, Ahonen teaches,

A method for maintaining secure network connections [see *Fig.1-5 and abstract;* and for example, *par.0004-0011*], the method comprising: duplicating, at a third network element [see *server/correspondent node 4 in Fig.4*], information associated with a secure network connection between a first network element and a second network element [see *Fig.2-3; where in Phase 1 and 2, par.0047 and 0088, the ISKAMP SA is negotiated between mobile host 1 and firewall 3 first, and the negotiation process is repeated between mobile host 1 and correspondent host 4*; and for example, *abstract, par.0001, 0005-0011, 0037, 0096-0099 and 0108-0129*], wherein a lookup of security associations associated with the secure network connection is not dependent on any destination address [*the Remote Control Database/RCDB is within the firewall, is not dependent on the destination address*; see for example, *par.0012, 0106, 0119-0122*].

Ahonen teaches replacing the security gateway with the correspondent node [*communication between mobile and correspondent host through the security gateway/firewall 3 is disclosed as "preferable";* see for example, *par.0004-0015; a separate negotiation process between mobile host and correspondent node is established;* see for example, *Fig.2-3; and par.0047 and0088; furthermore, during mobile host's remote access to intranet 5 in Fig.1, the server/correspond host may replace the firewall/security gateway 3*; see for example, *par.0108, 0146 to0156*]; but fails to disclose in response to detecting failure of the second network element, replacing the second network element with the third network element in the secure network connection with the first network element.

However, **Coile** teaches replacing the second network element with the third network element in the secure network connection with the first network element in response to detecting failure of the second network element [see FIG.1 and abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify the system of **Ahonen** by incorporating the teaching of **Coile** in order to implement a replacement for the function of a failed network device with a backup network device, so that network communication is not interrupted [see at least abstract of **Coile**].

As per Claim 11, Ahonen-Coile combination teaches,

sending at least one secure message from the third network element to the first network element [see *Fig.2-3; where in Phase 1 and 2, par.0047 and 0088, the ISKAMP SA is negotiated between mobile host 1 and firewall 3 first, and the negotiation process is repeated between mobile host 1 and correspondent host 4*; and for example, *abstract, par.0001, 0005-0011, 0037, 0096-0099 and 0108-0129 of **Ahonen***] to notify the first network element that the secure network connection will be taken over by the third network element [see abstract and **Backup Network Device 120** in Fig.1 of **Coile**].

As per Claim 20, Ahonen-Coile combination teaches,

during life of the secure network connection between the first and second network elements, the third network element receiving information relating to one or more security associations of the secure

network connection from the second network element [see *Fig.1 and abstract of* ***Ahonen****;* and for example, *par.0001, 0007 and 0008; where the third network element; i.e., correspondent host receives information about the SAs from the second network element; i.e., the firewall*].

As per Claim 21, Ahonen-Coile combination teaches,

the second and third network elements are security servers [see *security gateway 3 and correspondent node/server in Fig.1;* and for example, *par.0035 of* ***Ahonen***].

Claim 12, 14, 17 and 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over "Ahonen", in view of Atarashi et al. (US 6,173,312 B1 – "Atarashi")

As per Claim 12, Ahonen teaches,

A method for maintaining secure network connections [see *Fig.1-5 and abstract;* and for example, *par.0004-0011*], the method comprising: configuring a security gateway [see *firewall/Security Gateway 3 in Fig.*1] such that a lookup of security associations is not dependent on any destination address [*the Remote Control Database/RCDB is within the firewall, is not dependent on the destination address*; see for example, *par.0012, 0106, 0119-0122*]; and sharing at least one security association with security gateway [see *abstract and Fig.1-4; where a security association is shared between the firewall, the mobile and correspondent hosts*].

Ahonen does not explicitly disclose plurality of security gateways and sharing security association among the plurality of security gateways. However, in the same field of endeavor, **Atarashi** plurality of security gateways and sharing security association among the plurality of security gateways [see abstract and Fig.1 – *where plurality of servers and gateways, such as:* ***ROUTERS 101, 111, 121*** *are disclosed*].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention, to modify the system of **Ahonen** by adding one or more security gateways and

share SAs of among plurality of security gateways as taught by **Atarashi** in order to enhance the communication system, so that the function of a failed server would be protected by switching communication among servers [see col.2, line 43 to col.3, line 19 of **Atarashi**].

As per Claim 22, Ahonen-Atarashi combination teaches,

A first security server [see *Security Gateway/firewall 3 in Fig.1 of* ***Ahonen***. See also **WORKING SERVER 112** in FIG.1 of **Atarashi**]; and communicate with the mobile client using the at least one security association over the secure network connection between the first security server and the mobile client [*communication between mobile and correspondent host through the security gateway/firewall 3 is disclosed as "preferable";* see for example, *par.0004-0015; a separate negotiation process between mobile host and correspondent node is established;* see for example, *Fig.2-3; and par.0047 and 0088; furthermore, during mobile host's remote access to intranet 5 in Fig.1, the server/correspond host may replace the firewall/security gateway 3*; see for example, *par.0108, 0146-0156* of **Ahonen**].

Ahonen combined with **Atarashi** discloses a transceiver as a means for receiving information relating to at least one security association of a secure network connection between a mobile client and a second security server [see for example, *par.0019-0024 of* ***Ahonen*** *and* ***INPUT/OUTPUT PORT 340*** *in FIG.3 of* ***Atarashi***].

Ahonen does not explicitly disclose a processor module to monitor operation of the second security server; and in response to detecting failure of the second security server, send a message to the mobile client that the first security server is taking over the secure network connection. However, **Atarashi** discloses a processor module to monitor operation of the second security server [see ***NETWORK SUPERVISING APPARATUS*** *102 in Figs.1 and 3*]; and in response to detecting failure of the second security server, send a message to the mobile client that the first security server is taking over the secure network connection [see **BACKUP SERVER 122** in Fig.1; and for example, see col.2, line 43 to col.3, line 19].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicant's invention to incorporate the network supervising apparatus of **Atarashi** into the VPN of **Ahonen** in order to monitor and enhance the security system by adding additional servers as a backup, so that communication would not be interrupted.

As per Claim 14, Ahonen-Atarashi combination teaches,

wherein a lookup of security associations is not dependent on any destination address [*the Remote Control Database/RCDB is within the firewall, is not dependent on the destination address*; see for example, *par. [0012], [0106], [0119] to [0122] of* ***Ahonen***].

As per Claim 17, Ahonen-Atarashi combination teaches,

wherein communications between the first network element (mobile client) and the second network element (first security server) are based on a security architecture for the internet protocol (IPsec) [see *SAs based on IPSec in Fig.2 and 4 of* ***Ahonen***].

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2139)

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139